

# METHODS AND SYSTEM FOR DEFEATING TCP SYN FLOODING ATTACKS

## Abstract

Methods and a system for defeating TCP SYN flooding attacks  
5 are disclosed. In a server running TCP the invention assumes  
that, whenever receiving a SYN message, the server computes an  
ISR (Initial Sequence number Receiver side) and includes it in  
its SYN-ACK response to the client. Then, the server, also  
listening for the receiving of ACK messages from clients, checks  
10 the ISR. If checking fails, ACK message is dropped. If passing  
checking, ISR is accepted as an authentic computed ISR and  
decoded accordingly. Only then, resources are allocated and a TCP  
connection is actually established, after which, listening state  
is returned to in order to keep processing all received TCP  
15 messages.

Invention manages to allocate server resources to establish  
a TCP connection only when a client indeed completes the regular  
TCP 3-way handshaking procedure thus, preventing half-open  
connections created e.g., by DoS and DDoS attacks, from hogging  
20 server resources.